REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION (du bloc)	**CRITÈRES D'ÉVALUATION**

Définir et formaliser les besoins de sécurité des systèmes d'information	*Identifier et collecter les enjeux de la sécurité d'un système d'information en prenant en compte toutes les dimensions (technique, organisationnelle, humaine, juridique, réglementaire) de la problématique SSI.* **Compétence 1.1** : Identifier les problématiques de sécurité spécifiques à un système d'information sous l'aspect technique et organisationnel. **Compétence 1.2** : Poser les questions pertinentes sur la sécurité d'un système d'information afin de capturer au mieux les besoins auprès des différents interlocuteurs. **Compétence 1.3** : Recenser les contraintes d'ordre technique, organisationnel, juridique et réglementaire pouvant impacter la SSI. *Mener, de manière formelle, l'analyse de risque d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité.* **Compétence 1.4** : Identifier et définir les besoins de sécurité propres à un système d'information complexe. **Compétence 1.5** : Mener une analyse de risque complète, de manière rationnelle, sur un système complexe. Mettre en pratique une méthode d'analyse de risque (par exemple la méthode EBIOS). **Compétence 1.6** : Rédiger, en respectant le formalisme retenu, les documents synthétisant les besoins de sécurité, les menaces, les objectifs de sécurité. *Conseiller ou convaincre un donneur d'ordre (autorité, chef de projet, chef DSI…) dans le domaine de la SSI*. **Compétence 1.7** : Présenter une analyse de sécurité à un non-expert en SSI et le convaincre. **Compétence 1.8** : Synthétiser les documents formels sous la forme de fiches brèves accessibles à un non-expert, ne conservant que les points saillants (risques résiduels, points durs techniques, impacts opérationnels).	Exercices (écrits ou oraux) qui portent sur les enjeux de sécurité d'un système d'information. Évaluation du candidat sous la forme d'une mise en situation d'analyse de risque (réalisée en groupe) avec restitution des résultats (sous forme orale). Enfin le candidat effectue une mise en situation professionnelle (sur plusieurs mois) sur un sujet SSI, dont la problématique contient une composante technique importante, et donnant lieu à la rédaction d'un mémoire et d'une soutenance orale devant un jury. Ce dernier est composé d'experts SSI, de représentants de divers ministères, et de responsables de la formation.	Le candidat doit faire preuve : d'exhaustivité sur le traitement du sujet, de finesse d'analyse et d'esprit critique (par exemple, impact réel d'une problématique de sécurité dans le contexte d'emploi). Par ailleurs, lors de la restitution de la mise en situation d'analyse de risque, le candidat doit montrer : - qu'il a bien compris la démarche - qu'il a pris les décisions pertinentes et justifié ses choix d'une manière convaincante. On évalue également la qualité de la restitution de son analyse. Par ailleurs, on estime que le candidat est apte à conseiller et convaincre un donneur d'ordre si : - il comprend les enjeux métiers (crédibilité) - son discours est cohérent dans la restitution de son analyse - il répond convenablement aux questions posées par des interlocuteurs de différents niveaux - est convaincant.

Élaborer un dispositif technique correspondant aux besoins de sécurité	*Identifier et préciser les risques liés à un système d'information. Analyser les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques.* **Compétence 2.1** : Identifier et recenser sur un système d'information les principes et les mécanismes mis en œuvre pouvant remettre en cause les besoins de sécurité. Identifier les vulnérabilités techniques, identifier les menaces exploitant ces vulnérabilités, applicables au système d'information étudié. **Compétence 2.2** : Mettre en œuvre ou faire mettre en œuvre de manière appropriée les mécanismes de sécurité, notamment en définissant les contraintes d'installation, de configuration et d'utilisation. **Compétence 2.3** : Analyser les vulnérabilités d'un système d'information et en dégager les causes. Porter un regard critique sur un système informatique et sur ses mécanismes de sécurité, afin d'évaluer le niveau de risque et de faire des propositions d'amélioration. *Établir une architecture et définir un ensemble de solutions techniques pour protéger un système d'information selon des besoins de sécurité connus et selon les grands axes de la défense en profondeur. Faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information.* **Compétence 2.4** : Etudier la satisfaction des besoins dans les mécanismes de sécurité mis en œuvre. Proposer des équipements et des dispositifs (techniques ou non) pour réduire les risques pour le système d'information en fonction des besoins de sécurité identifiés. **Compétence 2.5** : Appliquer le principe de défense en profondeur (notamment selon les 5 axes : prévenir, bloquer, limiter, détecter, réparer) dans une architecture de sécurité. **Compétence 2.6** : Améliorer la sécurité d'un système informatique dans son ensemble et dans chacune de ses différentes composantes. **Compétence 2.7** : Concevoir et faire appliquer les bonnes pratiques.	Le candidat est évalué sur ses compétences en cryptographie, sécurité des systèmes, et des réseaux au moyen d'examens écrits et de questions orales portant sur des sujets techniques en SSI. Le candidat effectue également un mini-projet en sécurité logicielle. Enfin le candidat effectue une mise en situation professionnelle (sur plusieurs mois) sur un sujet SSI, dont la problématique contient une composante technique importante, et donnant lieu à la rédaction d'un mémoire et d'une soutenance orale devant un jury.	Le candidat doit identifier et préciser les risques liés à un système d'information, en particulier : - répondre correctement aux questions théoriques et pratiques qui lui sont posées dans les domaines de la cryptographie, de la sécurité des systèmes et des réseaux - exposer les principes généraux mis en œuvre dans le fonctionnement des systèmes d'information, et notamment dans les mécanismes permettant d'assurer la sécurité - identifier les limites des mécanismes de sécurité (défense en profondeur, exhaustivité,…). Par ailleurs, on vérifie que le candidat juge de manière fine les forces et les faiblesses des produits mettant en œuvre des mécanismes cryptographiques. Lors de la présentation orale, on évalue le candidat selon : - la qualité de restitution des travaux (auprès d'un spécialiste) sur des problématiques SSI ; il doit en particulier exposer la gravité des impacts qui peuvent en découler - la pertinence des propositions techniques et qu'il propose, en particulier, lorsqu'il s'agit de concevoir et faire appliquer des bonnes pratiques.

Estimer ou faire estimer le niveau de sécurité d'un système d'information	*Estimer soi-même le niveau de sécurité d'un système d'information.* **Compétence 3.1** : Identifier les vulnérabilités d'un système d'information, notamment par l'emploi d'outils. **Compétence 3.2** : Juger du niveau de sécurité d'un système d'information sur la base d'une analyse de son architecture, des composants le constituant, et des informations obtenues par audits et inspections. **Compétence 3.3** : Utiliser des outils d'audit. **Compétence 3.4** : Rédiger un rapport sur l'audit mené, recensant les vulnérabilités identifiées et proposant des mesures accompagnées d'une analyse d'efficacité. *Diriger et préparer un audit. Prendre en compte les résultats d'un audit. Élaborer et conduire un plan d'action.* **Compétence 3.5** : Définir et faire appliquer une stratégie d'audit. **Compétence 3.6** : Appliquer de manière pertinente les recommandations émises à la suite d'un audit, après en avoir analysé l'efficacité et les conséquences opérationnelles. **Compétence 3.7** : Elaborer un plan d'action. *Élaborer une démarche d'homologation et bien la conduire.* **Compétence 3.8** : Définir une démarche d'homologation détaillée et rédiger le dossier associé. **Compétence 3.9** : Conduire une démarche d'homologation conformément à un plan établi, et en restituer l'avancement et les résultats dans des documents formels. **Compétence 3.10** : Conseiller l'autorité d'homologation.	Réalisation d'audits sous forme de travaux pratiques. L'objectif est de superviser la réalisation d'un audit technique, d'organiser et choisir différentes prestations d'audit (type de prestation, contour retenu, etc.). Les candidats doivent ensuite appliquer la méthodologie d'audit, ainsi que des méthodes plus détaillées selon les domaines. On évalue également les candidats par le biais de la réalisation d'un mini-projet sur une étude de cas portant sur une analyse de risque et une homologation (avec restitution orale).	Le candidat est évalué selon : - la pertinence des outils choisis, leur utilisation et l'interprétation des résultats - le bon suivi de la réalisation des audits lors des travaux pratiques - le choix de la méthodologie d'audit adaptée à la situation - la connaissance et le respect de la réglementation Lors de la restitution orale de l'analyse de risque, on vérifie que le candidat : - a bien compris la démarche d'homologation et son inscription dans le paysage règlementaire français - a conduit correctement un processus d'homologation, de la constitution du dossier avec la compréhension de chacune des pièces qui le compose jusqu'à la prise de décision d'homologation, l'argumentaire qui y est associé et les conséquences d'une telle décision.

Gérer la sécurité d'un système d'information	*Contribuer à maintenir la sécurité d'un système, en relation avec les acteurs du projet, les spécialistes informatiques, les administrateurs et les RSSI.* **Compétence 4.1** : Identifier les acteurs d'un projet, leur rôle et leurs besoins. **Compétence 4.2** : Sensibiliser à la SSI, à un niveau approprié, chacun des acteurs identifiés. **Compétence 4.3** : Situer une action SSI et agir dans le cycle de vie d'un projet de manière pertinente. *Veiller sur les dernières vulnérabilités, menaces et produits de sécurité et les analyser. Évaluer les impacts d'une vulnérabilité ou d'une menace.* **Compétence 4.4** : Veiller sur les évolutions techniques, technologiques, les offres de produits et de services dans le domaine de la SSI, ainsi que sur les nouvelles menaces. **Compétence 4.5** : Porter un regard critique et pertinent sur des articles publiés ou des communications dans le domaine de la SSI. **Compétence 4.6** : Analyser l'impact de nouvelles vulnérabilités sur le système d'information considéré, ainsi que l'efficacité et les impacts opérationnels des éventuelles contre-mesures proposées. *Gérer un incident de sécurité*. **Compétence 4.7** : Faire appliquer la réglementation et les bonnes pratiques dans la gestion des incidents. **Compétence 4.8** : Mettre en place des mesures pertinentes pour limiter les impacts d'un incident.	Le candidat est évalué sur la réalisation d'un mini-projet sur le thème « management de la sécurité » et sa restitution orale. Le candidat doit écrire et soutenir à l'oral une étude bibliographique sur une vulnérabilité liée à la SSI, identifiée par des articles scientifiques et/ou grand public (les sources d'information sont majoritairement en anglais).	Le candidat est évalué selon : - son attitude face à la découverte d'un incident - sa réactivité et sa gestion de la crise - la pertinence de la démarche et des solutions qu'il propose. Le candidat doit : - identifier les différents acteurs d'un projet - sensibiliser ses interlocuteurs aux problématiques SSI - réagir face à des questions ou des oppositions - agir dans le cycle de vie d'un projet SSI de manière adaptée. Par ailleurs, le candidat doit également : - restituer avec finesse les problématiques liées à des vulnérabilités identifiées - proposer d'éventuelles contre-mesures - porter un regard critique et pertinent sur les réactions potentielles (de la presse par exemple), issues des publications de vulnérabilités dans le domaine de la SSI - adapter son discours concernant les impacts potentiels de la vulnérabilité identifiée en fonction du niveau de compétence en SSI des interlocuteurs auxquels il s'adresse.